

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)3 Electronic Devices in Possession of the Federal
Bureau of Investigation

Case No.

3:19mj50047

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 USC s. 846	conspiracy to distribute and possess with intent to distribute controlled substances
21 USC s. 841(a)(1)	possession with intent to distribute/distribution of controlled substances

The application is based on these facts:

Attached Affidavit of Michael T. Fuller

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 TFO FBI
Applicant's signature

Michael T. Fuller, TFO of the FBI

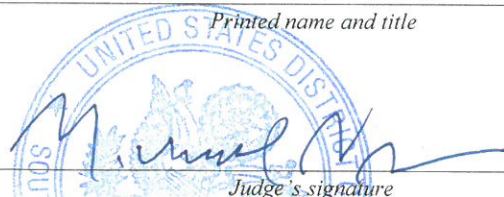
Printed name and title

Sworn to before me and signed in my presence.

Date:

8/14/19

City and state: Dayton, Ohio


Judge's signature

Michael Newman, US Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT DAYTON

IN THE MATTER OF THE SEARCH OF:
1) Gold Apple iPhone cellular telephone with
no external markings.
2) White and silver Apple iPhone SE Model
A1723 IMEI: 356605080447127.
3) White and gold Apple iPhone SE Model
A1662 IMEI: 353790081634098.
CURRENTLY LOCATED AT 7747 Clyo
Road, Centerville, Ohio 45459.

Case No. 3:19 mj 500 47

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Michael T. Fuller, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) within the meaning of Title 21, United States Code (U.S.C.), Section 878. That is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 21 U.S.C. § 878.

3. I am employed as a Police officer with the City of Dayton, Ohio and have been since 2001. I am currently assigned to the FBI – Cincinnati Division, Dayton Resident Agency and am a member of the Southern Ohio Safe Streets Task Force (SOSSTF). As such, I am charged with investigating crimes against the United States of America, including but not limited to violations of Title 18 and Title 21 of the United States Code. I have received training in drug trafficking investigations and have participated in numerous narcotics-related investigations (ultimately leading to successful prosecution) that involved surveillance, gathering evidence of money laundering, interviewing suspected drug traffickers, and supervising the activities of informants who provided information and assistance which resulted in the seizure of narcotics. I am familiar with federal drug laws, and am aware that it is a violation of Title 21, United States Code, Sections 841(a)(1) and 846 to distribute and possess with intent to distribute controlled substances, as well as to conspire to do the same. Further, I am aware of federal firearm laws and know that possessing firearms in furtherance of a drug trafficking crime is a violation of Title 18, United States Code, Sections 924(c)(1)(A) and 2. Since 2009, I have been dedicated solely to the investigation of narcotics offenses.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched:
 - a. Gold Apple iPhone cellular telephone with no external markings.
 - b. White and silver Apple iPhone SE, Model A1662, IMEI: 356605080447127.
 - c. White and gold Apple iPhone SE, Model A1662, IMEI: 353790081634098.

hereinafter referred to as “Devices.” The Devices are currently located at 7747 Clyo Road, Centerville, Ohio 45459.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On July 1, 2019, at approximately 3:30 p.m., Dayton Police Sergeant Ryan T. Halburnt, observed a black 2019 Chevrolet Camaro with extremely dark window tint driving towards him at a high rate of speed as he traveled south on N. Gettysburg Avenue at Edison Street. Sergeant Halburnt, who was driving a marked City of Dayton police cruiser, turned around as the vehicle passed him in an effort to read the license plate. The driver of the Camaro, later identified as Jamal BRASSFIELD, made a sudden left turn onto Kammer Avenue and began to accelerate away from Sergeant Halburnt as he traveled westbound through the residential neighborhoods.

8. Sergeant Halburnt notified members of the SOSSTF and their aerial support, who were in the area on an unrelated operation. The SOSSTF aerial unit located the black Camaro and relayed its' location until Dayton Police Officers Mark Orick and Ross Nagy were able to get behind it in their marked City of Dayton police vehicle. Officer Orick used his overhead lights to signal a traffic stop on the Camaro as they traveled northbound on State Route 49. The Camaro immediately accelerated away from the police cruiser in an effort to evade Law Enforcement.

9. The Camaro continued to drive at a high rate of speed through various neighborhoods until it eventually pulled into the Marathon Gas Station located at 4351 Riverside Drive. The driver and sole occupant, Jamal BRASSFIELD, exited the vehicle and went into the gas station. When he exited the gas station TFO Michael Fuller, TFO Fred Zollers, and Special Agent Nick Graziosi took him into custody.

10. The Chevrolet Camaro was inventoried prior to its' tow and a loaded Glock Model 36 handgun, \$8,980.00 in United States currency and 247 grams (field weight) of Marijuana were recovered from the passenger compartment of the vehicle. Investigators also seized 3 cellular telephones from BRASSFIELD's vehicle during the inventory:

- a. Gold Apple iPhone cellular telephone with no external markings.
- b. White and silver Apple iPhone SE, Model A1662, IMEI: 356605080447127.
- c. White and gold Apple iPhone SE, Model A1662, IMEI: 353790081634098.

11. Given the amount of marijuana and U.S. Currency in the vehicle, the presence of a firearm (a common tool of the drug trade), and his flight from police, I believe that

BRASSFIELD was engaged in drug trafficking activity. I know that drug traffickers frequently use cellular telephones like the Devices to contact customers, to arrange drug sales including price, quantity, and location, to take and send pictures of their products as well as conspirators. Drug traffickers frequently store videos and photographs on their cellular telephone relating to their drug trafficking activities, such images of themselves holding firearms, processing drugs, or displaying drug trafficking proceeds. Cellular telephones often contain information reflecting locations that a drug trafficker frequents or travels; this information may reveal locations of customers, stash houses, or sources of supply.

12. The Devices are currently in the lawful possession of the FBI Dayton Resident Agency. The Devices came into the FBI's possession in the following way: The Devices were seized incident to arrest by the Dayton Police Department and the FBI. Therefore, while the FBI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

13. The Devices are currently in storage at the FBI Dayton Resident Agency located at 7747 Clyo Road, Centerville, Ohio 45459. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal

computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and provide internet access. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.


CONCLUSION

20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

21. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Michael T. Fuller
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on August 14, 2019:

UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

1. The property to be searched:
 - a. Gold Apple iPhone cellular telephone with no external markings.
 - b. White and silver Apple iPhone SE, Model A1662, IMEI:
356605080447127.
 - c. White and gold Apple iPhone SE, Model A1662, IMEI:
353790081634098.

The devices currently stored at 7747 Clyo Road, Centerville, Ohio 45459.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 21 U.S.C. § 843(b) (use of a telecommunication facility to facilitate a controlled substance offense) and involve Jamal BRASSFIELD since February 1, 2019, including:

- a. lists of customers and related identifying information;
- b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- d. any information recording BRASSFIELD's schedule or travel from February 1, 2019 to the present;
- e. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.